BONNEVILLE POWER ADMINISTRATION

BPA Policy 236-13

Overview of Electronic Information Systems

Compliance and Governance

Table of Contents

236-13.1 Purpose & Background

A) This policy provides an overview for the media and systems available at BPA for storing and managing information assets in electronic formats.

B) BPA uses multiple electronic systems to manage and store information assets in support of BPA's business functions. Policies are required to ensure all information assets stored or managed on the types of electronic systems outlined in this chapter comply with the business objectives for information assets listed in BPA Policy 236-1 Information Governance & Lifecycle Management.

236-13.2 Policy Owner

The Executive Vice President of Compliance, Audit, and Risk Management has overall responsibility for this policy. The Agency Records Officer within Agency Compliance and Governance develops, implements and manages this policy on behalf of the Executive Vice President of Compliance, Audit, and Risk Management.

236-13.3 Applicability

A) This policy sets requirements for the use of BPA's Electronic Information Systems.

B) The focus of this policy is on systems that save information assets to, or interact with, the agency's primary and secondary servers. This policy applies to the following systems capable of storing and maintaining electronic information:

1) Electronic Records Management Systems (ERMS) and Electronic Recordkeeping Systems (ERKS)
2) Structured Electronic Information Systems (SEIS)
3) SharePoint sites
4) Shared/Network Drives
5) Personal Network Drives
6) Desktops/Laptops (Hard Drives)
7) "Near-line" Data Storage (flash/thumb drives, CDs, optical discs, diskettes, etc.)
8) "Offline" Data Storage (backup tapes, disaster recovery tapes, etc.)

C) Policies specific to each type of system will be detailed in BPA Policy 236-200 series. In addition to these electronic information systems (EIS) there are other systems that are considered communications tools (such as email), but may also be capable of storing data and recorded information. An overview of those systems is contained in BPA Policy 236-14 Overview of Communication Tools. All electronic information systems are subject to BPA's Code of Conduct and BPA Policy 434-4 Use of Government Equipment and BPA Information Technology Architecture (BITA).

236-13.4 Terms, Definitions & Acronyms

A) As used in this policy, the following terms and definitions apply:

1) **Agency File Plan**: The systematic method of identifying specific types of records maintained, series descriptions, and disposition authorities. The Agency File Plan maps to the Large Aggregate Flexible Schedule approved by NARA for BPA.

2) **Cloud Computing**: Computing services provided over the internet (or "cloud"), whereby shared resources, software, and information are provided to computers and other devices on demand.

3) **Electronic information**: Recorded information in electronic format (requiring computer technology to retrieve or access); digital content. This definition includes both the content of the information asset and its associated metadata.

4) **Electronic Information System (EIS)**: Computerized/digital means for collecting, organizing, and categorizing information to facilitate its preservation, retrieval, use, and disposition.

5) **Electronic Media**: The physical formats on which electronic information may be stored; this includes diskettes, videotapes, CDs, DVDs, optical discs, and other similar formats. It does not include hard drives, servers, or web-based access to electronic information. Data stored on Electronic Media is often referred to as "in-flight" data.

6) **Electronic Recordkeeping System (ERKS)**: See Structured Electronic Information System (SEIS); any SEIS that is substantially compliant with either DoD 5015.2 or F1000 standards for integrity, security, and disposition.

7) **Electronic Records Management System (ERMS)**: BPA's cross-agency, electronic recordkeeping system (ERKS). The system in which Federal records are collected and categorized to facilitate their preservation, retrieval, use, and disposition.

8) **Federal Record**: All recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Materials made or acquired solely for reference, extra copies of documents preserved only for convenience of reference and stocks of publications are not included. - see Federal Records Act, 44 USC §3301.

9) **Inactive Records**: A record that is no longer being used or updated for agency business functions, but has not exceeded its retention schedule (therefore not eligible for disposition). Inactive records may be archived so that they are not immediately accessible in order to reduce storage costs, but must still be appropriately organized and secured. Inactive transitory recorded information and short-term records will be automatically removed according to the general retention periods for these types.

10) **Information Asset**: Recorded information that has business value for BPA and must be managed throughout its lifecycle.

11) **Information Asset Plan**: Used to identify the file series for which an organization has been identified as being “Office of Record” in the Agency File Plan. The outline also contains additional information about the medium, location and other aspects of each organization’s information assets

12) **Metadata**: Structured information about any recorded information such as date and time the recorded information was created, the author, organization, or other data. This also includes descriptions of content, structure, data elements, interrelationships, and other characteristics of the data, information and records as well as information asset profiles or indexing data.

13) **Microfilm/Microfiche**: A film that contains images in greatly reduced form, typically requiring machine technology to view the images.

14) **Offer to NARA**: Permanent records offered to NARA and determined by NARA on a case-by-case basis whether historical retention is appropriate. BPA relinquishes all ownership and responsibility of these records. Permanent records are clearly marked in the Agency File Plan.

15) **Office of Record**: The organization which, by definition of its mission or function, that has primary responsibility for maintenance and retention of the record.

16) **Permanent Records**: A record that NARA has determined to have sufficient historical, administrative, legal, fiscal, or other value to warrant continuing preservation. See also TEMPORARY RECORDS.

17) **Personal Files**: Also called “personal papers,” documentary material belonging to an individual not used to conduct agency business. Personal files are excluded from the definition of Federal records and are not owned by the Government. - 36 CFR 1220.18.

18) **Short-Term Record**: Information assets that may provide some evidence of the agency’s organization, functions or activities, but are in an incomplete or draft form. Short-term records have a retention period of no more than two years.

19) **Structured Electronic Information System (SEIS)**: Electronic information systems (EIS) used by BPA to collect/maintain data or records in a structured format, typically a database. As part of the System Lifecycle (SLC) process, the IGLM team reviews and approves these systems for use at BPA. Electronic Recordkeeping Systems (ERKS) are a sub-set of SEIS that meet additional records compliance requirements.

20) **Temporary Records**: All records other than those offered to NARA for permanent retention. Those determined by the Archivist of the United States to

have insufficient value (on the basis of current standards) to warrant preservation by NARA. See also PERMANENT RECORDS.

21) **Transitory Recorded Information**: Recorded information with no continuing business value. This may also include recorded information made or acquired solely for reference, extra copies of documents preserved only for convenience and stocks of publications. Transitory recorded information has a retention period of no more than ninety days.

22) **Vital Records**: Those records that are essential to the continued functioning or reconstitution of BPA during and after an emergency including those records essential to preserving the legal and financial rights and interests of the organization and individuals directly affected by its activities as well as emergency operating materials key to maintaining the critical functions of the agency.

B) As used in this policy, the following acronyms apply:

1) **BITA**: BPA Information Technology Architecture

2) **COTS**: Commercial Off The Shelf

3) **DoD**: Department of Defense

4) **EIS**: Electronic Information System

5) **ERKS**: Electronic Recordkeeping System

6) **ERMS**: Electronic Records Management System

7) **IGLM**: Information Governance & Lifecycle Management

8) **NARA**: National Archives & Records Administration

9) **SaaS**: Software as a Service

10) **SEIS**: Structured Electronic Information System

11) **SLC**: System Lifecycle

236-13.5 Policy

A) Each of the EIS described in this chapter has certain features and functionality that make them more or less feasible for storing and managing an organization's information assets. Use of EIS should be determined based on the type of information assets the system will store or manage (i.e., transitory, short-term or Federal – including vital – records) with consideration for the integrity, security, and availability required for the material being stored and how the material must be managed throughout its lifecycle. The EIS policies in this chapter are outlined in order of preference for usage.

B) Organizations should be consistent in organizing and using EIS to support their business functions, reduce duplication, provide appropriate access to personnel, and manage the information assets for which they are responsible. This means assigning naming conventions and metadata that will identify the type of information assets being stored and (for Federal records) a way of identifying the file code for retention purposes. To assist in maintaining an inventory of the agency's Federal records, organizations are required to include the media and location of their records in an Information Asset Plan, which is submitted to the IGLM team (BPA Policy 236-12 Large Aggregate Flexible Schedule and Agency File Plan).

236-13.6 Policy Exceptions

A) Exceptions to this policy may be necessary based on legitimate business needs, legal or compliance requirements. Any exceptions must be documented, reviewed, and approved by the Office of Record, IGLM, and IT.

B) BPA allows for limited personal use of IT equipment (see BPA Policy 434-4 Use of Government Equipment). Employees may keep "personal papers" in electronic format such as benefits information, etc. on their hard drive or personal network drive. Any materials of this nature should be in folders marked "personal."

236-13.7 Responsibilities

A) **Agency Records Officer:** Manages the IGLM program and develops, issues, and enforces policies for managing BPA's information assets through their lifecycle to ensure compliance, reduce risk, and improve operational effectiveness and efficiency.

B) **IGLM Office:** Coordinates the overall IGLM program. Provides guidance and assistance to all BPA organizations with lifecycle management, and coordinates required records reviews, evaluations, and reports.

C) **Information Technology Office:** Manages and maintains BPA's electronic information systems to ensure the integrity, security, and availability of information assets.

D) **Managers/Supervisors:** Ensures the information assets their organization creates, maintains, and uses in support of their business function are managed in a consistent manner and are appropriately using the available electronic information systems.

E) **BPA Employees/Contract Personnel:** Manages information assets throughout its lifecycle by appropriately using the appropriate electronic information systems in a consistent manner to ensure integrity, security, and availability.

236-13.8 Standards & Procedures

A) **ERMS and Electronic Recordkeeping Systems (ERKS):**

1) ERMS is built on a SharePoint platform. It is addressed separately from SharePoint because it is the agency's only NARA-approved Electronic Recordkeeping System (ERKS), which is a system for storing Federal records that meets the DoD 5015.2 standard for records management. As such, it has been the priority means for maintaining BPA's electronic Federal records. ERMS only

contains final versions of inactive Federal records. However, ERMS is only capable of storing and managing electronic documents; it cannot store databases or similar applications. Therefore, certain Federal records may be maintained in Structured Electronic Records Systems (SEIS). Because BPA is implementing a successor ERKS to ERMS, it is currently not accepting new content. All ERMS content is scheduled for migration to the new system in 2016.

2) In addition to ERMS, Federal records may be maintained in an ERKS that has been reviewed and approved by IGLM as sufficiently meeting the DoD standard. BPA Policy 236-210 Structured Electronic Information Systems (SEIS) (*to be drafted*) contains the specifics of the DoD standard that BPA requires for approval of an ERKS.

B) **Structured Electronic Information Systems (SEIS):**

1) "SEIS" is typically used to describe commercial-off-the-shelf (COTS) or software-as-a-service (SaaS) systems (including "cloud computing") that manage data and information assets. This also includes enterprise applications such as PeopleSoft or Asset Suite. All SEIS must be scheduled with the IGLM team by completing form 1324.02e – Structured Electronic Information System Schedule. The form identifies the functional owner (who uses the system to support a business function) as well as the system owner (the IT organization that manages the system itself). In addition, inputs, data content, and outputs of the system are identified and scheduled for retention. Each SEIS is reviewed by the IGLM team for the integrity, security, and availability controls in place as part of the SLC process.

2) Because each SEIS is scheduled and has a metadata structure built in, data and information input to the system is a Federal record. However, by definition, these systems are not DoD 5015.2 compliant; therefore, the functional owner of the SEIS should consider providing outputs of the Federal records in a format that will meet the DoD standard. The IGLM team can provide guidance on appropriate formats and locations for maintaining these outputs through their lifecycle.

C) **SharePoint Sites:**

1) BPA uses Microsoft SharePoint® as both a means of internal communication and as a tool for organizations to share and manage their information assets. Although SharePoint generally meets the definition of SEIS, BPA uses SharePoint sites as a user-defined platform for managing organizations' information assets (i.e., organizations design, capture metadata, and populate their sites according to their specific business needs); therefore, SharePoint is addressed separately because of its unique usage throughout the agency.

2) SharePoint sites are preferred because of the increased availability of the material and reduction of duplication. However, these sites are only capable of storing and managing electronic documents; they cannot store databases or similar applications. In addition, organizations using the other functionalities available in SharePoint must determine if those functionalities are creating short-term or Federal records and implement a means for appropriately managing those records according to their retention periods as defined in the Agency File Plan.

3) Organizations must carefully consider access restrictions and define permission levels to ensure the continued security of the information assets managed on SharePoint sites. Each SharePoint site must have no more than two persons with the privileges to assign or restrict permissions to the site. Activating the version controls on the sites will assist in maintaining the integrity of the information assets as well. Organizations can contact the SharePoint Support team for additional guidance.

D) **Shared/Network Drives:**

1) Shared or network drives are an option for organizations to manage and share their information assets. They provide flexibility in arranging folders according to the organization's work needs, but they do not offer the same level of metadata that supports search, sharing and lifecycle management available with SharePoint or an SEIS. In addition, although access to folders can be restricted (through the Help Desk), most security features and metadata information currently need to be assigned to each document on an individual basis. Each organization should clearly document a shared/network drive record keeping procedure that addresses naming conventions, metadata, and retentions for the materials stored in them as part of their information asset plan.

E) **Personal Network Drives:**

1) Personal network drives shall not be used for work product because of the limited availability of information assets stored on these drives. In addition, use of these drives is likely to result in inconsistency or a lack of necessary metadata or categorization that is necessary for lifecycle management. (See NARA Bulletin on Shared Drives NARA 2012-02, 12/06/2011).

F) **Workstation PCs/Laptops (Hard Drive/Desktops):**

1) Hard drives (the "My Documents" folder) or the desktop location on workstation PCs and laptops are often used for initial drafts. However, any work-related information assets initially created or maintained on a hard drive/desktop shall be considered transitory recorded information and must be moved to a preferred storage location described in sub-sections 236-13.8 within ninety days and the appropriate metadata and retention schedule applied.

2) Laptops have an additional security risk because of the potential for loss or theft when taken offsite from BPA locations. Because laptops have virtual private network (VPN) capabilities allowing access to BPA network servers and SharePoint sites, most materials necessary for employees to accomplish their work is easily accessible. Therefore, laptop users should maintain only the minimum information assets on the laptop that is necessary to appropriately perform their responsibilities when offsite of the agency.

G) **"Near-line" Data Storage:**

1) Near-line data storage includes electronic media such as USB drives (also referred to as thumb drives or flash drives), CDs, DVDs, optical disks, diskettes, etc. They are generally considered to be those devices that store electronic information and require information technology to access. Because of their small size and portability, these devices should generally not be used to organize and maintain an organization's information assets. More specifically, USB drives are not to be used as the primary storage for Federal records.

2) Electronic media such as CDs, DVDs, and optical disks may be the best and most cost-effective means for maintaining Federal records (including vital records) when immediate availability is not required. If an organization determines to maintain Federal records in these media, the organization must document an inventory and a record keeping procedure that addresses naming conventions, metadata, and retentions for the materials stored in them.

H) **"Offline" Data Storage:**

1) These consist of backup tapes and disaster recovery tapes. Backup and disaster recovery tapes are the responsibility of the IT organization. They shall not be used by organizations as a means to maintain the information assets, particularly Federal records for which they are responsible.

236-13.9 Performance & Monitoring

A) The IGLM team within Governance and Internal Controls is the responsible organization for the performance standards and monitoring plans contained in this policy.

B) **Performance Standards**

1) Consistency in the organization and use of the agency's electronic information systems.

2) Reduced duplication, and increased accessibility of information assets by authorized users.

C) **Monitoring Plans**

1) Regular (at least tri-annual) review of information asset plans.

2) Regularly review of permissions for access to electronic information systems.

3) Regular compliance reviews of organizations’ information assets including categorization by the organization and metadata captured.

4) Monitoring through use of information technology.

236-13.10 Authorities & References

A) 18 USC 2071: Criminal sanctions for unauthorized removal/destruction of Federal records

B) 44 USC 3102: Establishing agency programs for management of, effective controls over, and appropriate disposal of records of temporary value

C) 44 USC 3105: Establishing safeguards against removal/loss of Federal records

D) 36 CFR 1220-1239: Federal Records Management, general

E) BPAM 1101: Information Technology Policies

F) BPA Policy 434-4: Business Use of BPA Information Technology Services

G) BPA Policy 236-1: BPA IGLM program authorization

H) DOE Order 0243.1: DOE records management directive

I) DOE 2015.2: Standard for systems maintaining Federal records

J) NARA Bulletin 2012-02: Guidance on managing content on shared drives http://www.archives.gov/records-mgmt/bulletins/2012/2012-02.html

236-13.11 Review

The IGLM team within Governance and Internal Controls is the responsible organization for this policy. This policy is reviewed on a three-year cycle beginning in 2015. All IGLM Manual policies are reviewed when revisions are introduced to BPA Policy 236-1 Information Governance and Lifecycle Management or other policies governing information management. Editorial updates to the policy and attachments may be made without IGOT and Policy Working Group review and approval.

236-13.12 Revision History

Version	Issue Date	Description of Change
2012-1	2012-11-05	Published completed original chapter, cmfrost.
2013-1	2013-09-03	Updated formatting, sect. 07, cmfrost.
2015-1	2015-08-07	Migration to new BPA policy format.